FEDERAL COURT OF AUSTRALIA

Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496

File number(s):	VID 556 of 2020
Judgment of:	**ROFE J**
Date of judgment:	5 May 2022
Catchwords:	**CORPORATIONS –** where respondent holds Australian Financial Services Licence – where respondent's business was targeted in cybersecurity attacks – whether respondent contravened ss 912A(1)(a) and (h) of the *Corporations Act 2001* (Cth) by failing to have adequate cybersecurity risk management in place – contraventions agreed by the parties – where parties prepared an agreed statement of facts and jointly proposed declarations and orders – whether proposed declarations and orders are appropriate – proposed declarations and orders made
Legislation:	*Australian Securities and Investments Commission Act 2001* (Cth) *Corporations Act 2001* (Cth) *Evidence Act 1995* (Cth) *Federal Court of Australia Act 1976* (Cth)
Cases cited:	*Australian Building and Construction Commissioner v Construction, Forestry, Mining and Energy Union* (2017) 254 FCR 68 *Australian Competition & Consumer Commission v Dataline.Net.Au Pty Ltd* (2007) 161 FCR 513 *Australian Competition & Consumer Commission v Dataline.Net.Au Pty Ltd* [2006] FCA 1427 *Australian Competition and Consumer Commission v Coles Supermarkets Australia Pty Ltd* [2014] FCA 1405 *Australian Competition and Consumer Commission v Cryosite* [2019] FCA 116 *Australian Securities and Investments Commission v AGM Markets Pty Ltd (in liq) (No 3)* (2020) 275 FCR 57 *Australian Securities and Investments Commission v Allianz Australia Insurance Limited* [2021] FCA 1062 *Australian Securities and Investments Commission v AMP*

	Financial Planning Pty Ltd (No 2) [2020] FCA 69 *Australian Securities and Investments Commission v Caddick* [2021] FCA 1443 *Australian Securities and Investments Commission v Camelot Derivatives Pty Ltd (in liq)* [2012] FCA 414 *Australian Securities and Investments Commission v Cassimatis (No 8)* (2016) 336 ALR 209; [2016] FCA 1023 *Australian Securities and Investments Commission v MLC Nominees Pty Ltd* [2020] FCA 1306 *Australian Securities and Investments Commission v RI Advice Group Pty Ltd (No 2)* [2021] FCA 877 *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2021] FCA 1193 *Australian Securities and Investments Commission v Westpac Banking Corporation (No 3)* [2018] FCA 1701 *Australian Securities and Investments Commission v Westpac Banking Corporation (No 2)* [2018] FCA 751 *Australian Securities and Investments Commission v Westpac Securities Administration Ltd* (2019) 272 FCR 170 *Hadgkiss v Aldin (No 2)* [2007] FCA 2069
Division:	General Division
Registry:	Victoria
National Practice Area:	Commercial and Corporations
Sub-area:	Regulator and Consumer Protection
Number of paragraphs:	93
Date of last submission/s:	14 April 2022
Counsel for the Plaintiff:	PW Collinson QC with PG Liondas and FL Shand
Solicitor for the Plaintiff:	Webb Henderson
Counsel for the Defendant:	KA O'Gorman
Solicitor for the Defendant:	Gilbert + Tobin

ORDERS

VID 556 of 2020

BETWEEN:	**AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION** Plaintiff
AND:	**RI ADVICE GROUP PTY LTD** Defendant

ORDER MADE BY: **ROFE J**

DATE OF ORDER: **5 MAY 2022**

THE COURT NOTES THAT:

1. In these Declarations and Orders, the following terms have the following meanings:

   (a) **AR** means authorised representatives (within the meaning of s 761A of the Corporations Act);

   (b) **Corporations Act** means the *Corporations Act 2001* (Cth);

   (c) **Licence** means Australian Financial Services Licence (**AFSL**) number 000238429; and

   (d) **RI Advice** means RI Advice Group Pty Ltd (ACN 001 774 125).

PURSUANT TO SECTION 21 OF THE FEDERAL COURT ACT AND SECTION 1101B OF THE CORPORATIONS ACT, THE COURT DECLARES THAT:

2. RI Advice contravened ss 912A(1)(a) and (h) of the Corporations Act from 15 May 2018 to 5 August 2021 as a result of its failure to have documentation and controls in respect of cybersecurity and cyber resilience in place that were adequate to manage risk in respect of cybersecurity and cyber resilience across its AR network, and as a result of this conduct, it:

   (a) failed to do all things necessary to ensure the financial services covered by the Licence were provided efficiently and fairly, in contravention of s 912A(1)(a) of the Corporations Act; and

   (b) failed to have adequate risk management systems, in contravention of s 912A(1)(h) of the Corporations Act.

AND THE COURT ORDERS THAT:

3. Pursuant to s 1101B of the Corporations Act:

   (a) RI Advice must engage Security in Depth (or such other cybersecurity expert as agreed between RI Advice and ASIC), to identify what, if any, further documentation and controls in respect of cybersecurity and cyber resilience are necessary for RI Advice to implement to adequately manage risk in respect of cybersecurity and cyber resilience across its AR network (**Further Measures**);

   (b) If as a result of the engagement referred to in paragraph 3(a), Further Measures are identified, RI Advice must in consultation with Security in Depth, agree upon the earliest reasonably practicable date by which RI Advice will implement the Further Measures (**Agreed Date**);

   (c) Within 30 days of the completion of the steps in paragraph 3(a), and if required paragraph 3(b), RI Advice must provide ASIC with a written report from Security in Depth, reporting as to whether Further Measures are required to be implemented, and if so, what the Further Measures are and the Agreed Date;

   (d) RI Advice must commence implementing the Further Measures by no later than 90 days from the engagement referred to in paragraph 3(a) and complete implementation by the Agreed Date; and

   (e) RI Advice must provide ASIC with a written report from Security in Depth, within 30 days after the Agreed Date reporting on the outcome of the implementation of the Further Measures, including whether, and to what extent, the Further Measures have been fully and appropriately implemented.

4. The engagement of Security in Depth referred to in paragraph 3(a) is to commence by no later than 1 month from the date of these Orders and RI Advice must provide Security in Depth with a copy of these orders prior to the commencement of the engagement.

5. The costs of Security in Depth and the implementation of any Further Measures are to be paid by RI Advice.

OTHER ORDERS

6. RI Advice pay a contribution to the plaintiff's costs of the proceeding fixed in the amount of $750,000.

7. The proceeding against the defendant is otherwise dismissed.

Note: Entry of orders is dealt with in Rule 39.32 of the *Federal Court Rules 2011*.

REASONS FOR JUDGMENT

ROFE J:

INTRODUCTION

1 The defendant (**RI Advice**) is the holder of Australian Financial Services Licence (**AFSL**) number 000238429 (the **Licence**) and is a financial services licensee within the meaning of s 761A of the *Corporations Act 2001 (Cth)* (the **Act**).

2 Pursuant to the Licence, RI Advice authorised independently-owned authorised representatives (**Authorised Representatives** or **ARs**) to provide financial services on RI Advice's behalf.

3 In the course of providing financial services pursuant to RI Advice's Licence, the Authorised Representatives electronically received, stored and accessed confidential and sensitive personal information and documents in relation to their retail clients.

4 Between June 2014 and May 2020, nine cybersecurity incidents occurred at practices of RI Advice's Authorised Representatives.

5 On 21 August 2020, the plaintiff (**ASIC**) commenced this proceeding by originating process and concise statement. In its originating process, ASIC sought declarations that RI Advice had contravened ss 912A(1)(a), (b), (c), (d), (h) and (5A) of the Act as a result of its failure to have and to have implemented, during specified time periods (including by its ARs), policies, plans, procedures, strategies, standards, guidelines, frameworks, systems, resources and controls which were reasonably appropriate to adequately manage risk in respect of cybersecurity and cyber resilience. ASIC also sought that RI Advice pay a pecuniary penalty under s 1317G(1)(a); and compliance orders under s 1101B(1)(a).

6 The concise statement was later replaced with a statement of claim, the final version of which amounted to over 250 pages.

7 The final hearing of the proceeding was fixed to commence on 4 April 2022. Prior to the commencement of the hearing I was informed that the matter had been settled.

8 On 7 April 2022 I received proposed declarations and orders to be made by consent, and an agreed statement of facts (**SAFA**) set out in **Annexure 1** of these reasons for judgment. Both parties have filed submissions in support of the proposed declarations and orders. In these documents, RI Advice admits to having contravened ss 912A(1)(a) and (h).

9 The evidence before the Court comprises the SAFA.

10 Having considered the SAFA and the parties' submissions I consider there to be a proper basis for making the proposed declarations and orders in the form agreed by ASIC and RI Advice. I now provide my reasons for doing so.

FACTUAL BACKGROUND

11 The following summary of the relevant facts is taken from the SAFA.

12 At all material times up to and including 30 September 2018, RI Advice was a wholly-owned subsidiary of Australia and New Zealand Banking Group Limited (**ANZ**). RI Advice was one of three ANZ financial licensees which from 1 October 2018 became part of the IOOF Holdings Limited (**IOOF**) group of companies (as it was then known).

13 RI Advice carries on a financial services business within the meaning of s 761A of the Act under a third-party business owner model. Under s 916A of the Act, RI Advice authorises independently-owned corporate authorised representatives and individual authorised representatives to provide financial services to retail clients on RI Advice's behalf and pursuant to the Licence. It does this in accordance with standard contractual terms between RI Advice and each Authorised Representative.

14 In the course of providing financial services pursuant to the Licence, the **AR Practices** (that is, practices of groups of one or more Authorised Representatives) electronically received, stored and accessed confidential and sensitive personal information and documents in relation to their retail clients. The personal information included:

(a) personal details, including full names, addresses and dates of birth and in some instances health information;

(b) contact information, including contact phone numbers and email addresses; and

(c) copies of documents such as driver's licences, passports and other financial information.

15 Since 15 May 2018, the AR Practices have provided financial services to at least 60,000 retail clients (although not concurrently).

16 Between June 2014 and May 2020, nine cybersecurity incidents occurred at AR Practices. They are detailed at [9] of the SAFA but in summary involved:

(a) an incident in June 2014 whereby an AR's email account was hacked and five clients received a fraudulent email urging the transfer of funds. One client made transfers totalling some $50,000;

(b) an incident in June 2015 where a third-party website provider engaged by an AR Practice was hacked, resulting in a fake home page being placed on the AR Practice's website;

(c) an incident in September 2016 where one client received an email requesting money, apparently from an employee of an AR Practice. The email was not sent by the employee and had been sent fraudulently. It came to light that the AR Practice used an email platform where information was stored "in the Cloud", meaning there was no anti-virus software and there was only one password which everyone used to access information.

(d) an incident in January 2017 where an AR Practice's main reception computer was subject to ransomware delivered by email, making certain files inaccessible;

(e) an incident in May 2017 where an AR Practice's server was hacked by brute force through a remote access port, resulting in file containing the personal information of some 220 clients being held for ransom and ultimately not recoverable;

(f) an incident where an unknown malicious agent gained unauthorised access to an AR Practice's server for a period of several months between December 2017 and April 2018 (**December 2017 Incident**). This event compromised the personal information of several thousand clients, a number of which reported unauthorised use of the personal information;

(g) an incident in May 2018 where an unknown person gained unauthorised access to the email address of an AR and sent a fraudulent email to the AR's bookkeeper requesting a bank transfer;

(h) an incident in August 2019 where an unauthorised person used an AR Practice's employee's email address to send phishing emails to over 150 clients; and

(i) An incident in April 2020 where an unauthorised person used the same email address as in the previous paragraph to send further phishing emails to the AR Practice's contacts.

17 The inquiries and reports made on behalf of RI Advice following the cybersecurity incidents revealed that, as at the dates of those incidents, there were a variety of issues in the respective ARs' management of cybersecurity risk. These included:

(a) computer systems which did not have up-to-date antivirus software installed and operating;

(b) no filtering or quarantining of emails;

(c) no backup systems in place, or backups not being performed; and

(d) poor password practices including sharing of passwords between employees, use of default passwords, passwords and other security details being held in easily accessible places or being known by third parties.

18 Prior to, and as at, 15 May 2018 (being the date on which RI Advice became aware of the December 2017 Incident, the most significant of the nine cybersecurity incidents), RI Advice had taken certain steps and had in place some documentation, controls and risk management measures in respect of cybersecurity risk for its ARs, including:

(a) training sessions, professional development events, and information provided through RI Advice's weekly newsletter for ARs;

(b) an incident reporting process where cyber incidents could be discussed; and

(c) obligations in the "Professional Standards" contractual terms between ARs and RI Advice relating to information security, electronic storage, incident notification requirements, fraud procedures and privacy.

19 The Professional Standards referred to above contained various recommendations and certain obligations designed to assist AR Practices in protecting client information from cybersecurity risks. These included password-protecting documents sent via email that contained clients' personal information; not using personal email addresses; using up to date security software; backing up data; and implementing a password policy.

20 RI Advice admits, that prior to and as at 15 May 2018, it did not have documentation, controls and risk management systems that were adequate to manage risk in respect of cybersecurity across its AR network.

21 Most of the historic issues were addressed by the significant improvements made by RI Advice to its existing cybersecurity risk management systems (after its acquisition by IOOF in October

2018), including taking steps to monitor and audit compliance with the cybersecurity requirements contained in RI Advice's Professional Standards. The improvements included engaging multiple external advisory firms to investigate past failures and review cybersecurity practices.

22 One of the initiatives undertaken by RI Advice was a program that IOOF designed during 2019 to increase awareness of cybersecurity and assist ARs in identifying and adopting cyber resilience good practices across all personal advice licensees within the IOOF group. This program was called the **Cyber Resilience Initiative**. IOOF engaged an external cybersecurity organisation, Security In Depth, to facilitate the Cyber Resilience Initiative and it was officially launched to ARs in January 2020.

23 The Cyber Resilience Initiative was implemented during 2020 and 2021 directly with the AR Practices. By 6 August 2021, the majority of AR Practices had implemented, and been approved (by Security in Depth) as having implemented to a good level, the majority of the best practices contained in RI Advice's Cyber Security Support Guide, which it had released to ARs in late 2019.

24 RI Advice admits, that whilst the measures it assessed and developed across the period of 15 May 2018 to 5 August 2021 in order to improve cybersecurity and cyber resilience for the ARs were designed to meet RI Advice's understanding of its obligations, it took too long to implement and ensure such measures were in place across its AR Practices. RI Advice accepts it should have had a more robust implementation of its program so that the measures were more quickly in place at each AR Practice and the majority of the AR network was confirmed as operating pursuant to such cybersecurity and cyber resilience measures earlier than 6 August 2021.

25 Since 5 August 2021, RI Advice has continued to implement the Cyber Resilience Initiative across the AR network.

RELEVANT PRINCIPLES

Consent orders in regulatory proceedings

26 The applicable principles regarding the making of orders by consent in regulatory proceedings, like the present one, were summarised by Gordon J in *Australian Competition and Consumer Commission v Coles Supermarkets Australia Pty Ltd* [2014] FCA 1405 ***(ACCC v Coles)*** as follows:

2.3.1 Orders sought by agreement

…

[70] The applicable principles are well established. First, there is a well- recognised public interest in the settlement of cases under the Act: *NW Frozen Foods Pty Ltd v Australian Competition & Consumer Commission* (1996) 71 FCR 285 at 291. Second, the orders proposed by agreement of the parties must be not contrary to the public interest and at least consistent with it: *Australian Competition & Consumer Commission v Real Estate Institute of Western Australia Inc* (1999) 161 ALR 79 at [18].

[71] Third, when deciding whether to make orders that are consented to by the parties, the court must be satisfied that it has the power to make the orders proposed and that the orders are appropriate: *Real Estate Institute* at [17] and [20] and *Australian Competition & Consumer Commission v Virgin Mobile Australia Pty Ltd (No 2)* [2002] FCA 1548 at [1]. Parties cannot by consent confer power to make orders that the court otherwise lacks the power to make: *Thomson Australian Holdings Pty Ltd v Trade Practices Commission* (1981) 148 CLR 150 at 163.

[72] Fourth, once the court is satisfied that orders are within power and appropriate, it should exercise a degree of restraint when scrutinising the proposed settlement terms, particularly where both parties are legally represented and able to understand and evaluate the desirability of the settlement: *Australian Competition & Consumer Commission v Woolworths (South Australia) Pty Ltd (Trading as Mac's Liquor)* [2003] FCA 530 at [21]; *Australian Competition & Consumer Commission v Target Australia Pty Ltd* [2001] FCA 1326 at [24]; *Real Estate Institute* at [20]-[21]; *Australian Competition & Consumer Commission v Econovite Pty Ltd* [2003] FCA 964 at [11] and [22] and *Australian Competition & Consumer Commission v Construction, Forestry, Mining and Energy Union* [2007] FCA 1370 at [4].

[73] Finally, in deciding whether agreed orders conform with legal principle, the court is entitled to treat the consent of [the defendant] as an admission of all facts necessary or appropriate to the granting of the relief sought against it: *Thomson Australian Holdings* at 164.

2.3.2 Declarations

[74] The Court has a wide discretionary power to make declarations under s 21 of the Federal Court Act: *Forster v Jododex Australia Pty Ltd* (1972) 127 CLR 421 at 437-8; *Ainsworth v Criminal Justice Commission* (1992) 175 CLR 564 at 581-2 and *Tobacco Institute of Australia Ltd v Australian Federation of Consumer Organisations Inc (No 2)* (1993) 41 FCR 89 at 99.

[75] Where a declaration is sought with the consent of the parties, the Court's discretion is not supplanted, but nor will the Court refuse to give effect to terms of settlement by refusing to make orders where they are within the Court's jurisdiction and are otherwise unobjectionable: see, for example, *Econovite* at [11].

[76] However, before making declarations, three requirements should be satisfied:

(1) The question must be a real and not a hypothetical or theoretical one;

(2) The applicant must have a real interest in raising it; and

(3) There must be a proper contradictor:

Forster v Jododex at 437-8.

Section 912A(1)(a) of the Act

27 As the holder of an AFSL, RI Advice is required to comply with the general obligations of a financial services licensee set out in s 912A of the Act. This includes the requirements:

(a) pursuant to s 912A(1)(a), to do all things necessary to ensure that the financial services covered by the Licence are provided efficiently, honestly and fairly; and

(b) pursuant to s 912A(1)(h), to have adequate risk management systems.

28 By reason of the broad standards prescribed by ss 912A(1)(a) and (h) of the Act, and the factual matters set out above, RI Advice admits that at all material times, it was required to:

(a) identify the risks that the ARs faced in the course of providing financial services pursuant to RI Advice's Licence, including in relation to cybersecurity and cyber resilience; and

(b) have documentation, controls and risk management systems in place that were adequate to manage risk in respect of cybersecurity and cyber resilience across the AR network.

29 The standard prescribed by s 912A(1)(a) of the Act has been considered in numerous decisions of this Court including by the Full Court in *Australian Securities and Investments Commission v Westpac Securities Administration Ltd* (2019) 272 FCR 170 at [169]–[175] (Allsop CJ), at [286], [289] (Jagot J), and at [421]–[427] (O'Bryan J) (***Westpac Securities***); and by Beach J in *Australian Securities and Investments Commission v AGM Markets Pty Ltd (in liq) (No 3)* (2020) 275 FCR 57 at [505]–[528] (***AGM Markets***).

30 The parties substantially agreed as to the relevant principles, subject to three matters discussed below. Those agreed relevant principles include:

(a) The phrase "efficiently, honestly and fairly" is to be read compendiously rather than as containing three discrete behavioural norms: *Australian Securities and Investments Commission v Camelot Derivatives Pty Ltd (in liq)* [2012] FCA 414 (***Camelot Derivatives***) at [69]; *Australian Securities and Investments Commission v Cassimatis (No 8)* (2016) 336 ALR 209; [2016] FCA 1023 (***Cassimatis***) at [674]; *AGM Markets* at [506]. To the extent that different views have been expressed as to whether the phrase

is to read compendiously, it is not necessary to resolve that issue for present purposes: see *Westpac Securities* at [424]–[426] (O'Bryan J)).

(b) Conduct may fail to meet the statutory definition even if it cannot be described as dishonest, and a breach of the standard is not limited to conduct that is "morally wrong in the commercial sense": *Westpac Securities* at [170] (Allsop CJ); *Australian Securities and Investments Commission v RI Advice Group Pty Ltd (No 2)* [2021] FCA 877 (***RI Advice (No 2)***) at [377]. Accordingly, acts or omissions can breach the statutory standard by reason of a failure by the licensee to act "efficiently and fairly", without there being a need also to prove a failure to act honestly: *Australian Securities and Investments Commission v Westpac Banking Corporation (No 2)* [2018] FCA 751 (***Westpac***) at [2352], [2360].

(c) A contravention of the "efficiently, honestly and fairly" standard does not require a contravention or breach of a separately existing legal duty or obligation, whether statutory, fiduciary, common law or otherwise. The statutory standard itself is the source of the obligation: *Westpac* at [2350]; *AGM Markets* at [512].

(d) It is well established that the words "efficiently, honestly and fairly" indicate that, amongst other things, the services are to be provided with "competence" in complying with relevant statutory obligations: *Camelot Derivatives* at [69]; *Cassimatis* at [674]; *Westpac* at [2347]–[2348]; *Westpac Securities* at [289] (Jagot J); *AGM Markets* at [507].

(e) In *Westpac Securities*, Allsop CJ said at [173] that the provision is part of the statute's legislative policy to require adherence to social and commercial norms or standards of behaviour. It follows that the boundaries and content of the relevant normative standard in any given case will be a matter for the Court to determine: eg, *Westpac* at [2532]; *RI Advice (No 2)* at [345].

(f) As for the requirement of "efficiency", this has been recognised as requiring that the licensee is "adequate in performance, produces the desired effect, is capable, competent and adequate": *Camelot Derivatives* at [69](c). In that same passage, Foster J gave an example: the efficiency requirement will not be met if the performance of a licensee's functions falls short of the "reasonable standard of performance… that the public is entitled to expect". There is some dispute as to the applicability of this passage, discussed further below.

(g) Accordingly, it is apparent that the obligation on a licensee under s 912A(1)(a) to ensure that the financial services provided on its behalf are provided "efficiently" imports a standard of reasonableness into the obligation. An example of a failure to act efficiently or fairly can be having inadequate procedures and training: *Westpac* at [27].

31 As noted above, RI Advice has raised three issues with ASIC's characterisation of the admitted contraventions of s 912A(1)(a).

Issue 1: "social and commercial norms"

32 RI Advice submits that its contravention admitted at [13] of the SAFA does not entail any breach of "social and commercial norms or standards of behaviour". RI Advice takes issue with ASIC's submissions, which it understands to allege such a breach.

33 RI Advice submits that there is no basis for a finding that "social and commercial norms" require any particular standard, or any particular system, for cyber risk management.

34 RI Advice submits that even if "social and commercial norms" were capable of having such application in this case, the SAFA does not:

(a) identify any relevant standard; or

(b) identify any basis on which any such standard could apply.

35 For that reason, RI Advice submits that when defining the standard of conduct that s 912A(1)(a) imposes and that was contravened in this case, it is not relevant to note, and there is no need to note, the extent that s 912A(1)(a) imposes an obligation in respect of "social and commercial norms or standards of behaviour".

36 The term "social and commercial norms or standards of behaviour" was used by Allsop CJ in *Westpac Securities* at [173]. It is useful to set out the whole passage, in which Allsop CJ describes the purpose of s 912A(1)(a):

> The provision is part of the statute's legislative policy to require social and commercial norms or standards of behaviour to be adhered to. The rule in the section is directed to a social and commercial norm, expressed as an abstraction, but nevertheless an abstraction to be directed to the "infinite variety of human conduct revealed by the evidence in one case after another". By the phrase itself, emphasis must be given to substance over form and the essential over the inessential in a process of characterisation by reference to the stated norm. Care needs to be taken that phrases used by judges in individual cases, in which they explain and articulate their views as to the success or failure in satisfying the norm in s 912A(1)(a), do not become rules to apply as defaults for the proper process of characterisation by reference to the words

> used by Parliament as to whether a body of conduct satisfied or failed to satisfy the norm.
>
> (Citations omitted.)

37 It is also useful to set out the one passage in ASIC's submissions in which they refer to the passage above:

> In *Westpac Securities*, Allsop CJ said that the provision is part of the statute's legislative policy to require adherence to social and commercial norms or standards of behaviour. It follows that the boundaries and content of the relevant normative standard in any given case will be a matter for the Court to determine…

38 I do not understand ASIC to submit that there has been a particular breach of a "social [or] commercial norm". The submissions do not use this language anywhere else, nor do they purport to identify any social or commercial norm it alleges to have been breached by RI Advice's conduct. ASIC referred to Allsop CJ's remarks in *Westpac Securities* in the course of its review of the relevant principles.

39 Furthermore, I do not understand the Chief Justice's remarks as going any further than providing an overview of the purpose of s 912A(1)(a). The remarks have not been used as a test or benchmark. Justice Beach in *AGM Markets* offered an alternative view, noting that neither of the other two members of the Full Court went so far, stating at [519]:

> With respect, I prefer to view s 912A(1)(a) as enshrining a statutory norm to be read conformably with s 760A and the other provisions of the *Corporations Act* and the *ASIC Act*, of course to be applied to an infinite variety of corporate delinquency and self-interested commerciality. But to say this is not to deny that it may implicitly pick up some aspects of what some might identify as social and commercial norms, although reasonable minds might differ as to where to ground such an otherwise free-floating concept.

40 There is no requirement in this case to determine the appropriateness of the "social and commercial norms" language, as I do not understand ASIC to be making such a case.

Issue 2: public expectations

41 RI Advice further submits that ASIC has incorrectly identified the relevant test for s 912A(1)(a) in issue in this proceeding, by using a test of public expectation.

42 ASIC's submissions relevantly state:

> As for the requirement of "efficiency", this has been recognised as requiring that the licensee is "adequate in performance, produces the desired effect, is capable, competent and adequate". If the performance of a licensee's functions falls short of the "reasonable standard of performance that the public is entitled to expect", then the efficiency requirement will not have been met. Accordingly, it is apparent that the

> obligation on a licensee under s 912A(1)(a) to ensure that the financial services provided on its behalf are provided "efficiently" imports a standard of reasonableness into the obligation. An example of a failure to act efficiently or fairly can be having inadequate procedures and training.
>
> (Citations omitted, emphasis added.)

43 RI submits that this demonstrates that ASIC has adopted the wrong test for determining whether the "efficiency" requirement in s 912A(1)(a) has been met, at least in cases in which the inefficiency concerns the inadequacy of risk management systems.

44 ASIC cites [69](c) of *Camelot Derivatives* in support of its submission. In that paragraph Foster J accepted as correct a submission that:

> The word "efficient" refers to a person who performs his duties efficiently, meaning the person is **adequate** in performance, produces the desired effect, is capable, competent and **adequate**: *Story v National Companies and Securities Commission* (1988) 13 NSWLR 661 at 672; 13 ACLR 225 at 234–5. Inefficiency may be established by demonstrating that the performance of a licensee's functions falls short of the reasonable standard of performance by a dealer that the public is entitled to expect: *Story v National Companies and Securities Commission* (1988) 13 NSWLR 661 at 679; 13 ACLR 225 at 241.
>
> (Emphasis added by RI Advice.)

45 RI Advice submits that in that paragraph Foster J makes clear that the relevant test is whether "the person is adequate in performance, produces the desired effect, is capable, competent and adequate". In the second part of the paragraph Foster J gives one possible illustration of how inefficiency may be established, by demonstrating performance falling short of "the reasonable standard of performance… that the public is entitled to expect". That is, Foster J uses that example to illustrate one way that the relevant test (ie, "the person is adequate in performance, produces the desired effect, is capable, competent and adequate") may be breached.

46 Cyber risks, an adequate response to such risks and building cyber-resilience requires appropriate assessment of the risks faced by a business in respect of its operations and IT environment. Cyber risk management is a highly technical area of expertise. The assessment of the adequacy of any particular set of cyber risk management systems requires the technical expertise of a relevantly skilled person.

47 Cyber risk management is not an area where the relevant standard is to be assessed by reference to public expectation. Rather, the adequacy of risk management must be informed by people with technical expertise in the area. I note that during the course of this litigation, both parties engaged highly qualified experts to produce reports outlining their opinions on the cybersecurity measures expected of an organisation like RI Advice. Some of this evidence is

referred to in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2021] FCA 1193. Further, the parties' proposed orders require the engagement of a cybersecurity expert to identify any further measures to be implemented in respect of cybersecurity and cyber resilience.

48 When Foster J gave as an example of a failure to meet the requirement of efficiency (or "inefficiency") a dealer's performance falling short of the reasonable standard of performance that the public is entitled to expect in [69](c) of *Camelot Derivatives,* he was not suggesting that the content of the standard is assessed by reference to the expectation of the public. Rather, he notes that the public is entitled to expect a reasonable standard of performance from a financial licensee.

49 Some conduct may be appropriate to assess through a public expectation lens: for example, fees charged for no service (like those in *Australian Securities and Investments Commission v MLC Nominees Pty Ltd* [2020] FCA 1306) or providing personal financial advice without consideration of the client's best interests (see *Westpac Securities*). While it may be said that the public would expect the holder of an AFSL to have adequate cybersecurity measures, this says nothing of the content. In a technical area such as cybersecurity risk management, the reasonable standard of performance is to be assessed by reference to the reasonable person qualified in that area, and likely the subject of expert evidence before the Court, not the expectations of the general public.

Issue 3: honesty and the compendious test

50 RI advice submits that, while it is accepted that the test in s 912A(1)(a) is "compendious", that does not mean that the contravention described in paragraph 2(a) entails a lack of honesty.

51 In ASIC's submissions, it notes that acts or omissions can breach the statutory standard by a licensee failing to act "efficiently and fairly", without a need to also prove a failure to act honestly. ASIC also notes that it has never alleged that RI Advice failed to act honestly with respect to cyber risks.

52 I understand this part of RI Advice's submissions to merely emphasise established principles and reiterate that ASIC does not allege, and RI Advice does not admit to, any conduct that lacked "honesty".

Section 912A(1)(h)

53 Section 912A(1)(h) of the Act requires the licensee to have "adequate risk management systems".

54 Although s 912A(1)(h) does not appear to have been the subject of any relevant prior judicial consideration, the notion of "adequacy" again imports a normative standard of conduct against which the licensee's performance can be judged. The particular focus of this provision is on "risk management systems", and in the context of RI Advice, whose business is conducted on its behalf through its Authorised Representatives, this necessarily places the focus on the risks to Authorised Representatives, and the necessity for RI Advice to have "adequate" systems to manage those risks.

55 The assessment of "adequate risk management systems", in the context of cyber risk management, requires consideration of the risks faced by a business in respect of its operations and IT environment. As I have noted above in relation to s 912A(1)(a), cyber risk management is a highly technical area of expertise. While the standard of "adequacy" is ultimately one for the Court to decide, the Court's assessment of the adequacy of any particular set of cyber risk management systems will likely be informed by evidence from relevantly qualified experts in the field.

DETERMINATION

Sections 912A(1)(a) and (h)

56 The factual background relevant to the contraventions is set out in the SAFA, which I accept as correctly setting out the relevant facts, some of which I have extracted above.

57 Cyberspace, and cyber-attacks, concern digital or computer technology or networks, and involve attacks directed at computers, computer systems or other information communication technologies. Cybersecurity is the ability of an organisation to protect and defend the use of cyberspace from attacks. Cyber resilience is the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber sources.

58 Risks relating to cybersecurity, and the controls that can be deployed to address such risks evolve over time. As financial services are increasingly conducted using digital and computer technology, cybersecurity risk has also increased. Cybersecurity risk forms a significant risk connected with the conduct of the business and provision of financial services. It is not possible

to reduce cybersecurity risk to zero, but it is possible to materially reduce cybersecurity risk through adequate cybersecurity documentation and controls to an acceptable level.

59 The AR Practices as providers of financial services were potential targets for cyber related attacks and cybercrime by malicious actors targeting Personal Information. That risk increased over time.

60 Since September 2018, RI Advice has engaged two external cybersecurity organisations to review cybersecurity in a sample of AR Practices, identify key best practice measures for RI Advice and its ARs, and monitor implementation of those measures.

61 Having regard to the above principles, and in the circumstances of RI Advice's financial services business as described above and as conducted on its behalf through its Authorised Representatives, I consider that the declarations regarding breaches of ss 912A(1)(a) and (h) are appropriate.

62 RI Advice admits that prior to and as at 15 May 2018, it did not have documentation, controls and risk management systems that were adequate to manage risk in respect of cybersecurity across its AR network.

63 The Cyber Resilience Initiative, designed by IOOF and implemented across 2020 and 2021 directly with the AR Practices (and by 6 August 2021 with the majority of AR Practices) had implemented, and been approved as being implemented, the majority of all the 11 best practices in the RI Advice Cyber Security Support Guide, to a good level.

64 However, RI Advice acknowledges that whilst the measures it assessed and developed across the period 15 May 2018 to 5 August 2021 in order to improve cybersecurity and cyber resilience for the ARs were designed so as to meet RI Advice's understanding of its obligations, it took too long to implement and ensure such measures were in place across its AR Practices. RI Advice accepts that it should have had a more robust implementation of its program so that the measures were more quickly in place at each of the AR Practices and the majority of the AR network was confirmed as operating pursuant to such cybersecurity and resilience measures earlier than 6 August 2021.

65 I find that from 15 May 2018 to 5 August 2021, RI Advice contravened s 912A(1)(a) of the Act in that it failed to do all things necessary to ensure that the financial services covered by its Licence were provided efficiently and fairly, by failing to ensure that adequate cybersecurity measures were in place and/or adequately implemented across its Authorised Representatives.

66 I find that from 15 May 2018 to 5 August 2021, RI Advice contravened s 912A(1)(h) of the Act in that it failed to have adequate risk management systems, by failing to implement adequate cybersecurity and cyber resilience measures and exposing its Authorised Representatives' clients to an unacceptable level of risk.

Declaratory relief

67 Section 21 of the *Federal Court of Australia Act 1976* (Cth) provides that, in civil proceedings in relation to a matter in which it has original jurisdiction, the Court may "make binding declarations of right, whether or not any consequential relief is or could be claimed". Accordingly, the Court may make declarations of contravention of provisions of the Act that are not civil penalty provisions. Section 1101B(1) of the Act provides an alternate basis on which to make declarations of admitted contraventions of s 912A(1) of the Act.

68 The Court has a wide discretionary power to make declarations bounded only by the limits of federal judicial power and the need to act judicially. The power is confined by the considerations which apply to the making of declarations generally, namely the three requirements set out by Gordon J at [79] of *ACCC v Coles* (extracted in full above):

(a) the question is a real and not a hypothetical one;

(b) the applicant has a real interest in raising the question; and

(c) there is a proper contradictor, that is a person who has a true interest to oppose the declaration sought.

69 It is well established that a statutory regulator, in discharging its function in the public interest, will have a "real interest" in bringing a proceeding and seeking appropriate declarations of contravention: *Australian Competition and Consumer Commission v Cryosite* [2019] FCA 116 (***ACCC v Cryosite***) at [38]. In particular, there is a real interest in the making of declarations of contraventions in light of the public interest in deterring contraventions of financial services laws, even where the contraventions arise primarily from careless omissions: *Australian Securities and Investments Commission v Allianz Australia Insurance Limited* [2021] FCA 1062 (***ASIC v Allianz***) at [121].

70 A defendant to a regulatory proceeding is a proper contradictor, even in circumstances where it has made admissions to the contravening conduct and agreed to the proposed orders, because it has an interest in opposing the declarations: *ACCC v Cryosite* at [39].

71 Declarations sought by regulators serve an important deterrent effect, by warning others of the risk of engaging in conduct giving rise to similar contraventions, and they record the Court's disapproval of the contravening conduct: *ASIC v Allianz* at [121]; *ACCC v Cryosite* at [40]. Declarations relating to contraventions of legislative provisions are similarly likely to be appropriate where they vindicate a regulator's claim that a party contravened the provisions, assist the regulator to carry out its duties, and deter other persons from contravening the provisions: *Australian Building and Construction Commissioner v Construction, Forestry, Mining and Energy Union* (2017) 254 FCR 68 at [93].

72 The form of the Court's declaration should specifically and succinctly identify the gist of the impugned conduct and its relationship to the contraventions in a concise way.

73 The agreed facts and admissions in the SAFA provide a sufficient factual foundation for the making of the declarations: s 191 of the *Evidence Act 1995* (Cth). Where there is a statement of agreed facts, evidence is not necessary to be adduced to prove the existence of the necessary facts which form the basis of the declarations: *Australian Competition & Consumer Commission v Dataline.Net.Au Pty Ltd* [2006] FCA 1427 at [57]–[59], endorsed by the Full Court in *Australian Competition & Consumer Commission v Dataline.Net.Au Pty Ltd* (2007) 161 FCR 513 at [92]; *Hadgkiss v Aldin (No 2)* [2007] FCA 2069 at [21]–[22]; *ACCC v Coles* at [79].

74 I consider that it is appropriate to make the proposed declarations for the following reasons.

75 First, RI Advice's admissions to the contravening conduct are set out in the SAFA, in particular at [10], [17], [18] and [25]–[27].

76 Second, the questions raised by the declarations are real and not hypothetical or theoretical.

77 Third, ASIC has a real interest in raising the questions that are to be the subject of the declarations. As a public regulator, it is in the interests of ASIC to seek the declarations concerning the application of s 912A(1), particularly in circumstances such as the present case, where the declarations may clarify to licensees that the relevant provisions of the Act also apply to the area of the management of risks in respect of cybersecurity. The declarations will serve to record the Court's disapproval of the contravening conduct, will assist ASIC to carry out its duties, and will deter other persons and entities from contravening the provisions as a result of similar conduct or omissions.

78 Fourth, the proceeding involves a matter of public interest, because it relates to contraventions of provisions of the Act that are primarily concerned with the protection of the public, and in particular the protection of consumers of financial services who may provide sensitive and/or confidential information to a financial services licensee or its Authorised Representatives.

79 Fifth, there is a proper contradictor. RI Advice as the entity who has contravened the Act, has an interest in opposing the relief, notwithstanding its admissions and agreement to the relief sought.

80 Finally, each of the proposed declarations discloses succinctly the basis upon which RI Advice's conduct has contravened ss 912A(1)(a) and (h) of the Act.

Orders under s 1101B of the Act

81 The proposed orders include compliance orders under s 1101B of the Act, which states:

> (1) The Court may make such order, or orders, as it thinks fit if:
>
> (a) on the application of ASIC, it appears to the Court that a person;
>
> (i) has contravened a provision of this Chapter, or any other law relating to dealing in financial products or providing financial services; or
>
> …
>
> However, the Court can only make such an order if the Court is satisfied that the order would not unfairly prejudice any person.

82 Section 1101B(1) of the Act confers on the Court a broad discretionary power. Section 1101B(4) provides a number of examples of the types of orders that the Court may make under s 1101B(1). Those examples are illustrative only and are not exhaustive of the orders that the Court may make: *Australian Securities and Investments Commission v Westpac Banking Corporation (No 3)* [2018] FCA 1701 (***Westpac No 3***) at [183]; *Australian Securities and Investments Commission v Caddick* [2021] FCA 1443 (***ASIC v Caddick***) at [316].

83 The power conferred on the Court by s 1101B(1) must be exercised judicially, having regard to the text, context and purpose of the Act: *Westpac No 3* at [183]. That purpose relevantly includes the protection of the public interest in the prevention of the conduct to which it relates and the importance of upholding public confidence in persons who might provide financial services to consumers: *ASIC v Caddick* at [322].

84 Further, that purpose may be served by forward-looking compliance orders under s 1101B aimed at ensuring specific deterrence in guarding against the possibility of the contravening

conduct happening again: *Australian Securities and Investments Commission v AMP Financial Planning Pty Ltd (No 2)* [2020] FCA 69 at [191], [238], [250].

85 The Court has power under s 1101B(1) to order the establishment of a compliance program including the appointment of an external expert. In *Westpac No 3*, Beach J made the following observations at [185]–[187] regarding orders for compliance programs under s 1101B:

> First, both s 1101B of the Corporations Act and s 12GLA of the ASIC Act confer a broad discretionary power. So much is evident from the text of s 1101B(1), which provides that the Court "may make such order, or orders, as it thinks fit". And whilst s 12GLA is drafted differently, the same point can be made. Moreover, I must consider whether such an order "is necessary in light of the particular circumstances of the contravention, other relief proposed to be granted, and in particular in light of any existing compliance program and steps taken since the contravention occurred": *Australian Competition and Consumer Commission v Renegade Gas Pty Ltd (t/as Supagas NSW) (2014) ATPR 42–485; [2014] FCA 1135 at [100(1)].*
>
> Second, the compliance program must have a connection with the contravening conduct that has been found: see *Australian Competition and Consumer Commission v Z-Tek Computer Pty Ltd (1997) 78 FCR 197 at 205; 148 ALR 339 at 347.*
>
> Third, I must strike the appropriate balance between prescription, so as to avoid uncertainty, and over particularity, so as to avoid unworkability *(Australian Competition and Consumer Commission v Virgin Mobile Australia Pty Ltd (No 2) [2002] FCA 1548 at [24] per French J).*

86 Paragraph 3 of the proposed orders provides for, among other things:

(a) the appointment of an external cybersecurity expert to identify what, if any, further documentation and controls in respect of cybersecurity and cyber resilience are necessary for RI Advice to implement to adequately manage risk in respect of cybersecurity and cyber resilience across its AR network (**Further Measures**); and

(b) the external expert to provide written reports to ASIC identifying:

  (i) what if any Further Measures are required to be implemented, and the agreed timeframe for the implementation of those measures; and

  (ii) the outcome of the implementation of any Further Measures within 30 days after the completion of the agreed timeframe,

87 It is appropriate that the Court make the proposed compliance orders for the following reasons.

88 First, given the circumstances of the contraventions, including RI Advice's admission that the inadequacies in its risk management systems in respect of cybersecurity and cyber resilience meant the ARs' clients faced an unacceptable level of risk up to 5 August 2021, it is appropriate

that an external expert now assess the adequacy of RI Advice's current documentation and controls in respect of cybersecurity and cyber resilience and assess whether any further measures are required.

89 Following 5 August 2021 (the latest date of the admitted contraventions), RI Advice has continued to implement the Cyber Resilience Initiative across the AR network. RI Advice acknowledges that it is appropriate that orders are made for the appointment of an external cybersecurity expert, Security in Depth (or such other cybersecurity expert as agreed between ASIC and RI Advice), as contemplated by the proposed compliance orders.

90 Second, the fact that RI Advice has made various improvements and extensions to its existing cybersecurity risk management systems in the period from 15 May 2018 to 5 August 2021, does not remove the need for an external expert to now assess the adequacy of its cybersecurity risk management systems. For example, in *Westpac No 3*, following the making of findings of contraventions of the *Australian Securities and Investments Commission Act 2001* (Cth) in respect of Westpac's Bank Bill Market trading during 2010, Beach J made orders in 2018 for Westpac to ensure that it had appropriate systems, policies and procedures in place in relation to Bank Bill Market trading and for the adequacy of those systems to be assessed by an independent expert. These orders were made notwithstanding ASIC had not identified any issue or concern with Westpac's current arrangements following substantial enhancements that Westpac had made to its policies, procedures and training since 2014: see *Westpac No 3* at [197] and [207]–[208].

91 Third, the purpose of the compliance program is tied directly to the conduct that is the subject of the declarations — that is, any documentation and controls in respect of cybersecurity and cyber resilience which are necessary for RI Advice to implement to adequately manage risk in respect of cybersecurity and cyber resilience across its AR network.

92 Finally, the orders are framed at an appropriate level of detail. In particular, the orders do not prescribe the further steps if any RI Advice is to take in respect of cybersecurity. Instead, the identification of any further measures is to be performed by the external expert. Similarly, the timeframe in which any further measures are to be implemented is not prescribed, but the earliest reasonably practicable date is to be agreed between RI Advice and the external expert once any further measures have been identified.

93 I will also make the proposed order as to costs and, subject to the foregoing, the dismissal of this proceeding.

I certify that the preceding ninety-three (93) numbered paragraphs are a true copy of the Reasons for Judgment of the Honourable Justice Rofe.

Associate: 

Dated: 5 May 2022

ANNEXURE A: STATEMENT OF AGREED FACTS AND ADMISSIONS

No. VID 556 of 2020

Federal Court of Australia
District Registry: Victoria
Division: General

Australian Securities and Investments Commission
Plaintiff
RI Advice Group Pty Ltd (ACN 001 774 125)
Defendant

NOTE: *The following statement of agreed facts and admissions is prepared pursuant to section 191 of the Evidence Act 1995 (Cth). The facts and admissions are agreed only for the purpose of this proceeding against the defendant (**RI Advice**).*

THE PARTIES

1 The plaintiff (**ASIC**) is:

(a) a body corporate under s 8(1)(a) of the *Australian Securities and Investments Commission Act 2001* (Cth) (the **ASIC Act**); and

(b) entitled to commence and maintain this proceeding in its corporate name under s 8(1)(d) of the ASIC Act.

2 The defendant:

(a) at all material times up to and including 30 September 2018 was a wholly-owned subsidiary of Australia and New Zealand Banking Group Limited (**ANZ**);

(b) was one of three ANZ financial advice licensees which from 1 October 2018 became part of the IOOF Holdings Limited (**IOOF**) group of companies (as it was then known);

(c) since 1 October 2018 has been a wholly-owned subsidiary of IOOF;

(d) is and at all material times was the holder of Australian Financial Services Licence (**AFSL**) number 000238429 (**Licence**) and a financial services licensee

(within the meaning of s 761A of the *Corporations Act 2001* (Cth) (the **Act**)); and

(e) is and at all material times was carrying on a financial services business (within the meaning of s 761A of the Act) under a third-party business owner model, meaning that it authorises independently-owned corporate authorised representatives and individual authorised representatives (within the meaning of s 761A of the Act) (**Authorised Representatives** or **ARs**) to provide financial services on RI Advice's behalf to retail clients pursuant to RI Advice's Licence (pursuant to s 916A of the Act) in accordance with standard contractual terms between RI Advice and each AR.

CYBERSECURITY RISKS FACED BY RI ADVICE'S ARs

3 At all material times, since 15 May 2018:

(a) RI Advice's ARs have provided financial services to clients pursuant to RI Advice's Licence, organised in practices of groups of one or more ARs (**AR Practices**); and

(b) there have been between about 89 and 119 AR Practices.

4 At all material times, in the course of providing financial services pursuant to RI Advice's Licence, the AR Practices received and stored and accessed, electronically, confidential and sensitive personal information and documents in relation to their retail clients (**Personal Information**), including:

(a) personal details, including full names, addresses and dates of birth and in some instances health information;

(b) contact information, including contact phone numbers and email addresses; and

(c) copies of documents such as driver's licenses, passports and other financial information.

5 Since 15 May 2018, the AR Practices have provided financial services to their clients which numbered at least 60,000 retail clients (although not concurrently).

6 Cyberspace, and cyber attacks, concern digital or computer technology or networks, and involve attacks directed at computers, computer systems or other information communication technologies. Cybersecurity is the ability of an organisation to protect and defend the use of cyberspace from attacks. Cyber resilience is the ability to

anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber sources.

7 Risks relating to cybersecurity, and the controls that can be deployed to address such risks, evolve over time. As financial services are increasingly conducted using digital and computer technology, cybersecurity risk has also increased. Cybersecurity risk forms a significant risk connected with the conduct of the business and provision of financial services. It is not possible to reduce cybersecurity risk to zero, but it is possible to materially reduce cybersecurity risk through adequate cybersecurity documentation and controls to an acceptable level.

8 By reason of the matters set out in paragraphs 4 and 5 above, at all material times, the AR Practices were potential targets for cyber-related attacks and cybercrime by malicious actors targeting Personal Information. That risk has increased over time.

9 Between June 2014 and May 2020, nine cybersecurity incidents occurred at AR Practices. These incidents involved:

(a) An incident in June 2014 involving an unknown party who appeared to have hacked an AR's Google email account and as a result five clients of the AR received an email which (fraudulently) appeared to come from the AR's email account, urging the transfer of funds to take advantage of an investment. One of the recipients was tricked into making transfers totalling about $50,000 to an account of one of the four major banks held by an unknown third party (approximately half of which was later recovered). This matter became the subject of a police investigation;

(b) An incident in June 2015 which involved a third-party website provider engaged by the AR, which hosted a knowledge centre website for that AR Practice, being hacked by an unknown third party. This resulted in a fake home page being placed on top of the knowledge centre website, such that the AR's clients could not get through to the AR Practice's own knowledge centre. Client Personal Information was not compromised;

(c) An incident in September 2016 which involved one client of an AR receiving an email requesting money which (fraudulently) appeared to have been sent from the email account of an employee of the AR Practice but was not sent by that employee. The client did not transfer the requested funds. The incident

occurred in the context where the AR reported that, at the time of the incident, the AR Practice used 'Microsoft Outlook 365', all of its information was stored 'in the Cloud' and that, as such, it had no anti-virus software installed on its systems; and there was one password which everyone in the practice used to access the information stored 'in the Cloud';

(d) An incident in January 2017 which involved an AR Practice's main reception computer being subject to ransomware delivered by email which resulted in certain electronic files being encrypted and made inaccessible on that computer;

(e) An incident in May 2017 which involved a server at an AR Practice being hacked by brute force through a remote access port, with files on that server being encrypted and the AR was requested to pay a ransom to make the files accessible. The files, which contained Personal Information of approximately 220 clients were not recoverable, but the AR Practice's IT advisers considered that the data had not been sent anywhere;

(f) An incident at an AR practice which was brought to RI Advice's attention in May 2018, in which an unknown malicious agent obtained (through a brute force attack) and then retained unauthorised access to the AR Practice's file server for a period of several months from about 30 December 2017 to about 15 April 2018 before being detected, resulting in the potential compromise of Personal Information of several thousand clients and other persons, a number of which reported the unauthorised use of their Personal Information (for example, by unauthorised bank accounts being opened in their names) (**December 2017 Incident**). The malicious agent had installed various software on the AR's computer server, including to enable brute forcing, crypto currency mining, a virtual private network, peer-to-peer file sharing and other hacking capability. Prior to obtaining access to the file server, over a 10-day period in October 2017, there were 27,814 unsuccessful login attempts using 2,178 different usernames from 10 different countries. The December 2017 Incident occurred in the context where the AR's IT consultant subsequently identified that 90% of the desktops of the AR were identified as not having up-to-date antivirus software, there were no scheduled scans during the working week for antivirus software, no offsite backups had been performed, and passwords and other security details were found in text files on the server desktop;

(g) An incident in May 2018 in which an unknown person obtained unauthorised access to the email account of an AR and used that email account to send an email request to the AR's bookkeeper to transfer money to a Turkish bank account (which transfer was not made);

(h) An incident in August 2019 which involved an unauthorised person using an AR Practice's employee's email account to send phishing emails to over 150 clients in that employee's contact list which requested recipients to click on a link to Dropbox. The Dropbox folder contained a file that was capturing credentials of people who tried to access it by clicking on the phishing email. The unauthorised party had also set up new rules in the employee's email mailbox automatically directing all incoming emails so that incoming emails would not appear in the email Inbox; and

(i) An incident in April 2020 which involved an external person obtaining unauthorised access to an email account of the same AR referred to in paragraph 9(g) above, resulting in phishing emails being sent to that AR's contacts.

10 The inquiries and reports made on behalf of RI Advice following the above cybersecurity incidents revealed that, as at the dates of those incidents, there was a variety of issues in the respective ARs' management of cybersecurity risk. While the position differed from AR Practice to AR Practice, the issues included, for example:

(a) computer systems which did not have up-to-date antivirus software installed and operating;

(b) no filtering or quarantining of emails;

(c) no backup systems in place, or backups not being performed; and

(d) poor password practices including sharing of passwords between employees, use of default passwords, passwords and other security details being held in easily accessible places or being known by third parties.

11 Most of the historic issues referred to in paragraph 10 above were addressed by the significant improvements made by RI Advice as set out below in paragraphs 19 to 23.

OBLIGATION TO HAVE ADEQUATE RISK MANAGEMENT SYSTEMS IN RESPECT OF CYBERSECURITY RISK

12 At all material times, as the holder of the Licence, RI Advice was required:

(a) pursuant to s 912A(1)(a) of the Act, to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly; and

(b) pursuant to s 912A(1)(h) of the Act, to have adequate risk management systems.

13 By reason of the matters set out in paragraphs 2 to 12 above, at all material times, RI Advice was required to:

(a) identify the risks that the ARs faced in the course of providing financial services pursuant to RI Advice's Licence, including in relation to cybersecurity and cyber resilience; and

(b) have documentation, controls and risk management systems in place that were adequate to manage risk in respect of cybersecurity and cyber resilience across the AR network.

14 ASIC has not ever alleged that RI Advice as a Licensee failed to act "honestly" with respect to cyber risks and the security and resilience measures for its AR Practices. ASIC did allege however that RI Advice failed to meet the remainder of the obligations set out in paragraphs 12 and 13 above.

RI ADVICE'S RISK MANAGEMENT SYSTEMS IN RESPECT OF CYBERSECURITY RISK

15 Prior to and as at 15 May 2018 (being the date on which RI Advice became aware of the December 2017 Incident which was the most significant of the nine cybersecurity incidents referred to above) RI Advice had taken certain steps and had in place some documentation, controls and risk management measures in respect of cybersecurity risk for its ARs including:

(a) Training and awareness sessions and information provided at professional development events and via RI Advice's weekly newsletter provided to ARs;

(b) An incident reporting process and forums in which incidents, including cyber incidents, were reviewed and discussed, including the Risk Event Forum and Event Working Group Forum;

(c) Obligations contained in "Professional Standards", which apply to ARs pursuant to their contractual arrangements with RI Advice and which are available to ARs on the RI Advice intranet. The relevant Professional Standards were:

(i) the Information Security Standard (later called the Information Security Procedures) which was updated and renamed the Cyber Security Standard effective from April 2020;

(ii) the non-mandatory Electronic Storage Guide which then became the mandatory Electronic Data Storage Standard effective from January 2020;

(iii) the Incident Notification Standard;

(iv) the Fraud Standard and Procedures; and

(v) the Privacy Standard.

16 The Professional Standards referred to above included various recommendations and certain obligations designed to assist AR Practices in protecting client information from cybersecurity risks. For example, the Information Security Procedures released in February 2016 provided that ARs should password-protect documents sent via email which contained personal client information; avoid using personal email addresses like Gmail; use passwords for IT devices and implement a password policy; use up-to-date security software including anti-virus; assess software annually for currency and apply patches regularly; have an "acceptable use" policy for staff; back up data regularly, store backups securely, and test them regularly; and implement physical security requirements such as locking premises and having a clean desk policy.

17 RI Advice nevertheless acknowledges that prior to and as at 15 May 2018, it did not have documentation, controls and risk management systems that were adequate to manage risk in respect of cybersecurity across its AR network.

18 Compliance with the Professional Standards requirements by the AR Practices was not audited by RI Advice in the period up to 15 May 2018 beyond seeking confirmation from ARs that they had read and were aware of the Professional Standards. As at and from 15 May 2018 until 5 August 2021, RI Advice did not have in place adequate auditing and compliance mechanisms to provide assurance to RI Advice that the Professional Standards requirements relating to cybersecurity were understood by its ARs and were being met and, where they were not being met, risks or compliance actions were subsequently raised for RI Advice's management attention.

19 In the period from 15 May 2018 to 5 August 2021, RI Advice made various improvements and extensions to its existing cybersecurity risk management systems

including taking steps to monitor and audit compliance with the cybersecurity requirements contained in the Professional Standards. These improvements and steps were prompted by the December 2017 Incident which RI Advice learned of in May 2018 and included:

(a) In July 2018, engaging KPMG to conduct a forensic investigation in respect of the December 2017 Incident. KPMG's final report was issued on about 24 October 2018. The AR Practice worked with ANZ (prior to 1 October 2018), and subsequently IOOF, in the period up to September 2019 to address the recommendations contained in the report as to cybersecurity enhancements for the AR Practice;

(b) In September 2018, engaging Security In Depth, an external cybersecurity organisation, to conduct a review of a sample of AR Practices. In October 2018, Security In Depth provided a Report Synopsis which identified significant issues with managing and protecting client Personal Information, with similar issues identified across the sample AR Practices. These included, for example, poor password management, limited or poor use of multi-factor authentication, and limited or non-existent monitoring tools and services to detect if a malicious individual has gained access or still has access to internal systems, and no processes for managing a potential cybersecurity incident. Security in Depth concluded that if the issues observed with the sample AR Practices were a reflection on the AR's generally then significant change was urgently recommended;

(c) Also in or around September 2018, engaging Cyber Indemnity Solutions, a second external cybersecurity organisation, to conduct a review of two AR Practices to provide a direct comparison between Security In Depth and another provider. One of these reports also identified significant issues with managing and protecting client Personal Information;

(d) Working with Security In Depth to identify key measures which could be implemented as a priority to address cybersecurity risk for ARs, comprising password management, implementing multifactor authentication (**MFA**) and password protecting sensitive data sent by email (**Three Core Initiatives**). The Three Core Initiatives were communicated to the ARs in November 2018. In

May and June 2019, RI Advice confirmed to ARs that the Three Core Initiatives were mandatory and required ARs to attest to having implemented them. By 6 August 2019, all but six AR Practices had completed the attestations. By 3 September 2019, all but three AR Practices had completed the attestations and the three remaining AR Practices completed their attestations shortly thereafter;

(e) From February 2019, working with Security In Depth to review and update cybersecurity policies for the ARs. This resulted in a "Cyber Security Support Guide" being prepared and released to the ARs on 19 August 2019. It contained ten "best practices" to address cybersecurity risk. An updated version, containing an eleventh "best practice", was released to ARs in November 2019 and, at the same time, ARs were asked to have their technology providers review the Guide and confirm by email that the existing technology network met those standards. In April 2020 an attestation process was commenced through which ARs were required to attest to having implemented the 11 best practices. By the end of April 2020, 34 of about 121 AR Practices had attested to implementing the 11 best practices. The attestation process was discontinued in October 2020 as it was superseded by the Cyber Resilience Initiative (see below);

(f) From June 2019, auditing ARs' compliance with the requirement to have MFA enabled on Xplan. Full compliance had not yet been reached by April 2020 and RI Advice subsequently "forced" MFA centrally on Xplan for all users from 30 June 2020;

(g) From about August 2019, making a cybersecurity toolkit available to ARs via the RI Advice intranet;

(h) In October 2019, establishing an Advice Processes and Client Records program, which ultimately would require ARs to store all Personal Information in the Xplan database, including so that these records were held securely. Part of this program involved a process of ensuring that all records and client files held by the AR Practices for a certain number of years were scanned onto Xplan. This program was rolled out across the AR Practices in a phased approach, during 2019 through to 2021;

(i) In January 2020, releasing an updated Electronic Data Storage Standard which mandated that ARs use Xplan for the storage of all client files containing Personal Information;

(j) Working with IOOF's Professional Standards team and Security In Depth to prepare and release the Cyber Security Standard, which was effective from 14 April 2020 and which included various mandatory cybersecurity controls such as the requirements to patch software regularly, implement MFA for all systems and regular data backups;

(k) In April 2020, communicating a Cybersecurity Incident Response Plan Breach Process Guide to the ARs;

(l) Offering a cyber-specific insurance solution to the AR Practices from about February 2019, and commencing a requirement that new ARs have cybersecurity insurance from 1 October 2020; and

(m) In conjunction with the Cyber Resilience Initiative project team and Security In Depth, preparing and providing to ARs a template cyber security policy in January 2021.

The Cyber Resilience Initiative

20 During the course of 2019, IOOF designed a program to increase awareness of cyber security and assist ARs in identifying and adopting cyber resilience good practices across all personal advice licensees within the IOOF group (including RI Advice). This program was called the **Cyber Resilience Initiative**. IOOF engaged Security In Depth to facilitate the Cyber Resilience Initiative and it was officially launched to ARs in January 2020.

21 In summary, the Cyber Resilience Initiative comprised mandatory cybersecurity training and a mandatory assessment following completion of the training (all of which was completed by June 2020 for the ARs), followed by a cybersecurity assessment by Security In Depth of each AR Practice based on information provided by each AR in an online survey. Security In Depth assessed each AR Practice against the 11 best practices contained in the Cyber Security Support Guide which RI Advice had previously provided to its ARs.

22 In the period from about 18 August 2020 to about 23 July 2021, Security In Depth produced an initial report for each AR Practice which identified gaps against the 11

best practices. These initial reports identified that a significant number of ARs had not implemented one or more of the 11 best practices. Each AR Practice then had a period of six months to address those gaps, following which Security In Depth conducted a follow-up assessment and produced a second "close out report".

23 From about March 2021, Security In Depth provided a close out report for each AR Practice once all of the outstanding actions for the 11 best practices for that AR Practice had been notified as complete. By 6 August 2021, Security In Depth had provided a close out report for the majority of the AR Practices.

Implementation of cybersecurity measures across the ARs

24 RI Advice recognises that cyber risks and an adequate response to such risks and building resilience requires appropriate assessment of the risks faced by a business in respect of its operations and IT environment.

25 The Cyber Resilience Initiative was implemented across 2020 and 2021 directly with the AR Practices and by 6 August 2021 the majority of AR Practices had implemented, and been approved as having implemented, the majority of all the 11 best practices to a good level. RI Advice acknowledges that the further measures that RI Advice implemented for its ARs took too long.

26 That is, RI Advice acknowledges that whilst the measures it assessed and developed across the period of 15 May 2018 to 5 August 2021 in order to improve cybersecurity and cyber resilience for the ARs were designed so as to meet RI Advice's understanding of its obligations, it took too long to implement and ensure such measures were in place across its AR Practices. RI Advice accepts it should have had a more robust implementation of its program so that the measures were more quickly in place at each AR Practices and the majority of the AR network was confirmed as operating pursuant to such cybersecurity and resilience measures earlier than 6 August 2021.

CONTRAVENTION OF SECTIONS 912A(1)(a) AND (h) AND PROPOSED COMPLIANCE ORDERS

27 By reason of the matters set out in above, from 15 May 2018 to 5 August 2021 RI Advice:

(a) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently and fairly by reason of RI Advice's failures to comply with its

obligations referred to in paragraph 13 above by failing to ensure that adequate cybersecurity measures were in place and/or adequately implemented across the ARs from 15 May 2018 until 5 August 2021; and

(b) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraph 13 above, the risk management systems in respect of cybersecurity and cyber resilience meant the ARs' clients faced an unacceptable level of risk.

28 Following 5 August 2021, RI Advice has continued to implement the Cyber Resilience Initiative across the AR network. In the circumstances, the parties agree that it is appropriate that orders are made for RI Advice to engage Security in Depth (or such other cybersecurity expert as agreed between RI Advice and ASIC), to identify what, if any, further documentation and controls in respect of cybersecurity and cyber resilience are necessary for RI Advice to implement to adequately manage risk in respect of cybersecurity and cyber resilience across its AR network.

7 April 2022